Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 21 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports sixteen foreign−born construction workers with phony immigration documents were able to enter a nuclear weapons plant in eastern Tennessee because of lax security controls. (See item 1)
- The Associated Press reports federal agriculture officials have suggested steps to help school officials throughout Iowa find ways to protect school lunches from the threat of bioterrorism. (See item 11)
- The Washington Post reports Chinese farmers have tried to suppress major bird flu outbreaks among chickens with an antiviral drug meant only for humans, violating international livestock guidelines, and thus rendering the bird flu drug useless. (See item 18)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 20, Associated Press* — **Fake documents got workers into nuclear plant.** Sixteen foreign−born construction workers with phony immigration documents were able to enter a nuclear weapons plant in eastern Tennessee because of lax security controls, a federal report said Monday, June 20. Controls at the Y−12 weapons plant have since been tightened and there was no evidence the workers had access to any sensitive documents, said the National Nuclear

Security Administration, which oversees nuclear weapons facilities for the Department of Energy (DOE). However, the DOE inspector general's office said in the report issued Monday that its field agents found "official use only" documents "lying unprotected in a construction trailer which was accessed by the foreign construction workers" at the plant. "Thus, these individuals were afforded opportunities to access ... (this) information," the inspector general wrote. "We concluded that this situation represented a potentially serious access control and security problem." The report, initiated by a tip in 2004, said the workers had fake green cards that certified them to work in the United States. The Y−12 plant makes parts for nuclear warheads and is the country's principal storehouse for weapons−grade uranium. It is located in Oak Ridge, TN.
Inspector General's report: http://www.ig.doe.gov/pdf/ig−0691.pdf
Source: http://abcnews.go.com/US/wireStory?id=864758&CMP=OTC−RSSFeed s0312

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 20, Associated Press* — **One killed in explosion at oil storage facility.** One person was killed in an explosion and fire at an oil storage facility in Jackson County, GA. At least one of the storage tanks at Joe Sikes Oil Service exploded shortly after 10 p.m. (EDT) Sunday, June 19. Firefighters were able to get blaze under control after about 90 minutes. "We did some initial evacuations in the immediate area −− one neighborhood adjacent to the facility," Lt. Bobby Chaisson of the fire department in nearby Jefferson said after the fire was contained. The evacuation order was later lifted and police have begun investigating the cause of the fire.
Source: http://www.ajc.com/metro/content/metro/0605/20explosion.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *June 20, Associated Press* — **Study flags gaps in terrorism insurance.** Significant gaps in the nation's terrorism insurance program could slow efforts to revive the economy after future attacks, according to a study released Monday, June 20. Many insurance policies protect against foreign terrorists, but don't cover losses caused by homegrown terror groups or even attacks involving chemical, biological, nuclear or radiological weapons, which are among America's top threats, a report by Rand Corp. finds. Though scores of companies obtained coverage after a 2002 federal law freed up billions of dollars to help insurers pay claims, many businesses haven't bothered taking out policies. Terrorist coverage currently equals only half the amount of commercial assets protected by other insurance policies, said Bob Reville, co−author of the study. Without insurance, a terrorist strike could heavily damage the economy because businesses would have trouble rebuilding and hiring again.

Full Document and Summary available at:
http://www.rand.org/publications/MG/MG393/index.html
Source: http://abcnews.go.com/US/wireStory?id=864151

4. *June 17, TheHawaiiChannel.com* — **University of Hawaii warns students, faculty of potential identity theft.** Students and faculty who attended or worked at all 10 campuses of the University of Hawaii (UH) system are being encouraged to take steps to protect themselves against identity theft after a recent case involving a former library employee. Deborah Jenkins was employed at Manoa's Hamilton Library from 2001 until 2003. Until recently, the university system used Social Security numbers to keep track of who checked out library materials. As a library assistant Deborah Jenkins had access to those numbers. Jenkins and her husband, Paul, were indicted for identity theft and bank fraud last October. Authorities arrested the couple in Florida. Paul Jenkins admitted that he and other family members used the identity of a Maryland man, which he obtained in Florida, to apply for $48,000 in student loans. Authorities issued an arrest warrant on Deborah Jenkins. She remains at large, probably on the mainland. School officials said they are working with the U.S. Attorney's Office and Secret Service to determine whether the suspect used any of the information in UH's database for identity theft.
Source: http://www.thehawaiichannel.com/news/4622931/detail.html?rss =hon&psp=news

[Return to top]

Transportation and Border Security Sector

5. *June 20, Richmond.com (VA)* — **Virginia's new rail fund to provide $23 million of annual improvements.** Governor Mark R. Warner recently signed legislation creating the Rail Enhancement Fund, the first dedicated revenue stream for investment in rail infrastructure in Virginia's history. The Fund, which will be created on July 1, 2005, will support improvements for inter−city passenger, commuter, and freight rail throughout Virginia. Virginia's rail infrastructure is almost exclusively privately owned. There are 3,400 miles of rail track in Virginia, all of which are privately owned by freight railroads. Seventy−one percent of freight rail traffic hauled in Virginia is coal. The majority of freight in Virginia is through−traffic, bound for destinations outside the state. There are currently two passenger railroads in Virginia, VRE and Amtrak, which operate on approximately 616 miles of track. Projects will be selected by the Commonwealth Transportation Board based upon the recommendations of the Rail Advisory Board, which comes into existence on July 1, 2005, and will consist of nine members appointed by the Governor to four−year terms.
Source: http://www.richmond.com/news/output.aspx?ID=3733241&Vertical_ID=127&tier=10&position=1

6. *June 20, Associated Press* — **Massachusetts transit system to install more security cameras.** The Massachusetts Bay Transit Authority (MBTA) is keeping a close eye on its subway passengers. The transportation agency is moving ahead with plans to install more closed−circuit television cameras to enhance safety. MBTA General Manager Daniel Grabauskas says they're also building more "hub" systems that will allow transit workers to view the video feeds from remote locations.
Source: http://www1.whdh.com/news/articles/local/DBB1967/

7. *June 20, New York Daily News* — **Conductorless train gets failing grade.** Passengers and transit employees gave the Manhattan Transit Authority (MTA) a big thumbs−down on Sunday, June 19, as the conductorless L train rolled down the tracks on its maiden voyage. The Transit Authority began the controversial pilot program on Sunday at 12:01 a.m. (EDT), running the Canarsie−line train with only a motorman aboard the trains on weekends and late at night. Some MTA employees said the one−person operation −− which is expected to be expanded to all hours on the 24−station line by the end of the year −− isn't safe. A motorman for five years, train operator Gilbert Gonzalez said working without a conductor to monitor passengers and open and close the doors made him very uneasy. "If somebody was being robbed or was sick, I wouldn't know it," he said. For years, the MTA has run shorter trains on a handful of small shuttles without conductors. MTA spokesperson Mark Groce said trains in Chicago, Philadelphia and Paris successfully run with only drivers. However, MTA operator Haley Daley said she was afraid of being attacked when she drove a four−car train without a conductor. Daley, an operator for six years, said in case of emergency, it would be impossible for one person to evacuate a train.
   Source: http://www.nydailynews.com/front/story/320721p−274273c.html

8. *June 19, United Press International* — **U.S. security inspects Egyptian airport.** Officials from the U.S. Transportation Security Administration (TSA) inspected Egypt's Cairo International Airport Saturday, June 18, to ensure air travel security. Airport officials said a TSA team toured the terminals and luggage storage, as well as monitored the Egyptian security measures taken at Cairo Airport. They said the inspection was part of a U.S. campaign to monitor the security measures at international airports where flights are destined to the United States.
   Source: http://washingtontimes.com/upi/20050618−103526−5056r.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

9. *June 20, Agricultural Research Service* — **New tests screen weed for resistance to major herbicide.** Two rapid, nondestructive tests have been developed by Agricultural Research Service (ARS) scientists to screen a troublesome weed for resistance to the world's most−used herbicide. ARS scientists Clifford H. Koger III and Dale L. Shaner developed the test to determine if horseweed plants were resistant or susceptible to the herbicide glyphosate. In 2000, horseweed (Conyza canadensis) became the first weed species to develop resistance to glyphosate in cropland where glyphosate−resistant soybeans were grown. Glyphosate−resistant biotypes of horseweed have now been confirmed in 13 states east of the Mississippi River. Glyphosate is effective at killing all plant types including grasses, broadleaves and sedges, as well as perennial and woody plants. After emergence, glyphosate−resistant crops are capable of tolerating multiple applications of the herbicide, while weeds are killed. However, repeated use

over many years has left several weed species resistant to glyphosate. If glyphosate resistance is confirmed, the tests should help reduce the spread of resistant horseweed populations because growers will use different herbicides to manage the resistant weeds. Koger and Shaner are testing both assays to see if they're useful for screening other weed species for resistance to glyphosate.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

10. *June 20, Associated Press* — **Advisory on scab conditions now online.** Advisories about the plant disease known as scab can be found on the Web, courtesy of South Dakota State University (SDSU). The area covered has been expanded to include all of eastern South Dakota and a few adjacent counties in the west, according to Jeff Stein, small grains pathologist at SDSU. "Additionally, the advisory now covers both winter and spring wheat and could even be used to make decisions about other small grains such as barley," he said. The fungal disease, formally known as fusarium head blight, is linked to wet weather. The risk categories on the online advisory are based on weather at the time the crop is flowering, said Marty Draper, SDSU plant pathologist.
Scab advisories: http://plantsci.sdstate.edu/smallgrainspath/
Source: http://www.aberdeennews.com/mld/aberdeennews/news/11938874.h tm

[Return to top]

Food Sector

11. *June 20, Associated Press* — **Iowa schools work to protect school lunches.** School officials throughout Iowa are being encouraged to find ways to protect school lunches from the threat of bioterrorism. Federal agriculture officials have suggested the steps and part of follow up risk assessment since the terrorist attacks of September 11, 2001. Most schools already protect food, securing storage and preparation areas and having those areas inspected annually by experts. Many schools also limit the food students can share with classmates, experts said. In Des Moines, staff will get more training and officials will reassess how locks and other security measures are being used, said Teresa Nece, Des Moines schools' food services director. Recent programs offered over the Iowa Communications Network addressed school food safety issues for the first time in Iowa. The U.S. Department of Homeland Security, the U.S. Department of Inspections and Appeals, the Iowa Department of Education and Iowa State University Extension co−sponsored the recent program for school officials.
Source: http://www.wcfcourier.com/articles/2005/06/20/news/breaking_news/914f79928e7bf698862570260033fc07.txt

12. *June 20, USAgNet* — **Tuberculosis−exposed workers found in poultry plant.** About 100 workers are thought to have been exposed to the tuberculosis (TB) bacteria in a Marshall Durbin broiler processing plant in Jasper, AL. However, health officials said none of the have an active case of the disease and there is no threat to the public health. The 100 workers who tested positive for the TB bacteria at the plant have been given chest x−rays, state health official Karen Landers said. Tuberculosis, which is an airborne disease, cannot be contracted through food. State health workers gave skin tests to more than 200 employees who had worked closely with a former employee who tested positive for TB. "We have tested all the workers on the shift in which the person with the disease worked and there is no indication at this time that anyone

has the disease," Landers said.
Source: http://www.usagnet.com/story−national.cfm?Id=626&yr=2005

13. *June 17, Food Ingredients First* — **Rosen's Diversified, American Foods Group announce merger.** Rosen's Diversified, Inc. (RDI) and American Foods Group, Inc. have announced an agreement in principle to create a new national food company, "American Foods Group, LLC" by combining the operations of American Foods Group, Inc. and the Rosen Meat Group, Inc., a wholly owned RDI subsidiary. The new company, to be headquartered in Alexandria, MN, will consist of all of American Foods Group, Inc. current operations, along with RDI's meat processing companies. RDI's agricultural chemical distribution and fertilizer business units are not part of the agreement. The parties expect the merger to close by late August. Combined total sales for the two companies last year were over $1.5 billion.
Source: http://www.foodingredientsfirst.com/newsmaker_article.asp?id NewsMaker=8420&fSite=AO545&next=2

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

14. *June 20, Jakarta Post (Indonesia)* — **Four more polio cases confirmed in Indonesia.** Indonesian health authorities confirmed on Monday, June 20, that four more children have been infected with polio, bringing to 50 the total number of people who have contracted the disease in the country's first outbreak in a decade. Health Minister Siti Fadilah Supari told a press conference that all of the polio cases were confirmed in the West Java and Banten provinces. Siti explained that 24 out of 50 polio cases were detected in the Banten district of Lebak, while 18 others were confirmed in the West Java district of Sukabumi, where the first case was identified. Four other polio cases were detected in West Java district of Bogor, while two polio cases were confirmed in the districts of Cianjur and Serang. Georg Petersen, head of the World Health Organization (WHO) representative in Jakarta, said "more polio cases are expected" in Indonesia as the health ministry is still waiting the laboratory results of a number of cases of acute flaccid paralysis.
Source: http://www.thejakartapost.com/detaillatestnews.asp?fileid=20 050620162105&irec=2

15. *June 20, Moscow News (Russia)* — **West Russia hepatitis outbreak spreads to Moscow.** Seven Moscow, Russia, residents have been diagnosed with hepatitis A, the city’s chief sanitary inspector Nikolai Filatov told the press on Monday, June 20. Filatov said that all the victims contracted the disease in the town of Rzhev in the Tver region west of Moscow where at least 683 people have been diagnosed with Hepatitis A this summer. According to Russian media, health inspectors have blamed a Rzhev brewery for the outbreak. They say that the enterprise used contaminated water for producing soft drinks and this could have spread the illness. Representatives of the brewery have denied those accusations.

Source: http://www.mosnews.com/news/2005/06/20/hepatitismoscow.shtml

16. *June 20, Canadian Press* — **Scarcity of autopsies on bird flu victims blinds science to course of disease.** While at least 54 people have died from H5N1 infections since December 2003, autopsies have been performed on fewer than a handful of cases. For cultural and other reasons, body after body has been buried or cremated, robbing pathologists of the precious chance to chart the havoc the virus wrecks on its victims. "That's one of the reasons why it's so difficult to understand what the virus does in the body," says Klaus Stohr, who heads the World Health Organization's global flu program. "Post−mortems are important. But ... there are less than five done, I think, so far. And all in Thailand." Thailand hasn't reported a human case in the most recent wave of infections, which began in December 2004. That means science has no autopsy data with which to try to explain the worrisome changes in infection patterns that have observed over the last six months in Vietnam, changes which flu experts fear mean the virus is becoming more transmissible and more likely to spark an influenza pandemic. Without information that can only be gathered through autopsies, scientists devising treatment options and potential vaccines are working, if not in the dark, then in a dim light, experts say.
Source: http://www.canada.com/health/story.html?id=576770c7−9dcb−46b5−b186−a68966a98846

17. *June 19, Agence France Presse* — **Scientists find Severe Acute Respiratory Syndrome medicine.** Scientists conducting research in eastern China have found that a medicine used to treat schizophrenia is effective in treating patients with Severe Acute Respiratory Syndrome (SARS). Chinese and European scientists in eastern Hangzhou city found that cinanserin, used to treat mental illness since the 1970s, can inhibit the coronavirus that causes SARS. The drug was identified as the only ready−to−use medicine among 15 possible anti−SARS remedies recommended by scientists participating in the Sino−European Project on SARS Diagnostics and Antivirals (SEPSDA). "The finding means that cinanserin could be directly prescribed to prevent the SARS disease or treat SARS patients if the fatal epidemic mounts a comeback," Peter Kristensen, an academic from Denmark's University of Aarhus, was quoted saying. The three−year SEPSDA program is funded by the European Union and involves eight Chinese and European institutions. Launched in 2004, it aims to find 50 chemical compounds to treat SARS. Scientists working for the program also confirmed on Sunday the finding of two homologous SARS coronaviruses in animals from the Netherlands and Hong Kong respectively. Both the newly found viruses and the formerly detected SARS virus were variations of an ancient virus, which had been in animals for ages but remained unidentified, said Rolf Hilgenfeld, a professor from Germany's University of Luebeck.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050619/hl_afp/healthsarschina_050619112402

18. *June 18, Washington Post* — **Bird flu drug rendered useless.** Chinese farmers, acting with the approval and encouragement of government officials, have tried to suppress major bird flu outbreaks among chickens with an antiviral drug meant for humans, animal health experts said. China's use of the drug amantadine, which violated international livestock guidelines, was widespread years before China acknowledged any infection of its poultry, according to pharmaceutical company executives and veterinarians. The Chinese Agriculture Ministry approved the production and sale of the drug for use in chickens, according to officials from the Chinese pharmaceutical industry and the government, although such use is barred in the U.S.

and many other countries. Local government veterinary stations instructed Chinese farmers on how to use the drug and at times supplied it, animal health experts said. Amantadine is one of two types of medication for treating human influenza. But researchers determined last year that the H5N1 bird flu strain circulating in Vietnam and Thailand, the two countries hardest hit by the virus, had become resistant, leaving only an alternative drug that is difficult to produce in large amounts and much less affordable, especially for developing countries in Southeast Asia.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/17/AR2005061701214.html

19. *June 16, Howard Hughes Medical Institute* — **Fragment of yellow fever virus may hold key to safer vaccine.** In one of the first molecular studies of the human antibody response to yellow fever, Howard Hughes Medical Institute (HHMI) researchers and their colleagues have found the crucial bit of virus that people's immune systems need to spot and destroy this re−emerging disease. The findings may help scientists improve the existing vaccine, which has rare but severe side effects, said Jan ter Meulen, an HHMI research scholar and associate professor of virology at Leiden University Medical Center in The Netherlands. The group has identified a specific region on one of the viral proteins that elicits an immune response. Antibodies produced by the immune system interact with this part of the protein, known as a neutralizing epitope, to fight off infection. To protect people from the disease, yellow fever vaccines must contain this essential fragment of instruction to the immune system, said ter Meulen. Yellow fever strikes more than 200,000 people a year, mostly in Africa, killing about 30,000 of them, the World Health Organization estimates. No drug treatment is effective against the virus.
Yellow fever information: http://www.cdc.gov/ncidod/dvbid/yellowfever/index.htm
Source: http://www.hhmi.org/news/termeulen.html

[Return to top]

Government Sector

20. *June 20, Associated Press* — **Man shot at Seattle courthouse.** A man was shot inside Seattle, WA's downtown federal courthouse on Monday, June 20. The courthouse was evacuated after he walked inside the building and made threats, police said. The man entered the lobby of the 23−story federal building shortly before noon with what appeared to be a hand grenade, police spokesperson Christie−Lynne Bonner said. Police and federal agents responded and shot the man. Seattle police chief Gil Kerlikowske said the man appeared to be dead. He also said the suspect's backpack does not contain explosives. Fire department medics couldn't treat the man for more than an hour because the bomb squad had to make sure the backpack was safe. The World War 2−style grenade did not explode. U.S. Marshal Eric Robertson said the man was stopped before going through security. He was carrying a backpack and holding what appeared to be a grenade in his hand. The new federal courthouse opened last August. Many of the major security features of the $171 million high−rise are disguised. Even glass walls that permit ample sunlight are blast−resistant.
Source: http://www.cbsnews.com/stories/2005/06/20/national/main70310 2.shtml

[Return to top]

Emergency Services Sector

21. *June 20, The Intelligencer (WV)* — **West Virginia county to stage mock exercise.** The Harrison, WV, County General Health District will stage a mass mock exercise Wednesday, June 22, in conjunction with emergency units and agencies in the area to simulate a smallpox outbreak in the Cadiz area. The purpose of the drill will be to test the readiness of responding units and ensure an effective, systematic response should a disaster occur. . State and local emergency officials will evaluate each site and conduct an after−action review. Eric Wilson, bioterrorism response and training coordinator for the district, said that while the upcoming event is only a simulation, the possibility of attack or other disaster is quite real. "The path of Flight 93, which crashed in Somerset County, PA, went over Harrison County, Jefferson County and Brooke County," he said. Federal funding through a Public Health Infrastructure Grant is defraying all costs for the exercise.
Source: http://www.news−register.net/community/story/0620202005_com0 2.asp

22. *June 20, Federal Computer Week* — **California municipality adopts holistic approach to mesh networking.** The Northern California city of Ripon will deploy a municipal wireless network in the next several weeks to enable secure, high−speed voice and data communications among first responders and other city employees. Mesh networks are designed to be multihop systems in which any member device can transmit packets via the network. Ripon public works officials are planning to use the mesh network to monitor data from supervisory control and data acquisition, commonly known as SCADA systems, which collect data from sensors and machines and transmit them to a central computer. Ripon Police Chief Richard Bull said the city will use the network when it deploys more than 20 surveillance cameras to monitor and investigate suspected criminal activity. The cameras will be placed at three truck stops on a major freeway, in city parks and at locations in the downtown area, among other places. City officials have identified several additional uses for the wireless network, including giving police officers in patrol cars access to law enforcement and court databases, allowing police and firefighters to access an incident command system during emergencies, and enabling officials to transmit geographic information system data about hazardous material sites, fire hydrant locations and commercial building plans.
Source: http://www.fcw.com/article89302−06−20−05−Print

23. *June 19, CBS 5 (CA)* — **Hazmat drill to take place at California Air Force base.** Law enforcement and emergency response agencies will participate in a hazardous materials drill Friday, June 24, on Travis Air Force Base in Northern California. The exercise will test the emergency response capabilities of the agencies to a criminal attack involving a hazardous materials release within a residential neighborhood that causes mass casualties, said Paula Toynbee of the Solano County Sheriff's Department. Local police and fire agencies will join the Solano County Office of emergency Services in conducting the drill. Communication and coordination among the responding agencies will also be tested and evaluated. An estimated 200 responders will participate in the drill, Toynbee said.
Source: http://cbs5.com/localwire/localfsnews/bcn/2005/06/19/n/HeadlineNews/DRILL/resources_bcn_html

24. *June 19, Baltimore Sun (MD)* — **A simulated attack puts Maryland responders' emergency preparedness to the test.** A Terrorist Railway Attack Exercise in Carroll County, MD, on

Friday, June 17, depicted the chaos resulting from the bombing of a rail car tanker filled with 55 tons of anhydrous ammonia. The common industrial chemical is frequently transported by rail under pressure as liquid. When pressure drops, as it would after an explosion, the chemical reverts to gas. More than 150 volunteer emergency personnel took part in the drill, reacting to the simulated explosion and its aftermath. Fire and emergency personnel from 12 fire companies responded with aid for the victims and decontamination of the site. The drill involved the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the state fire marshal, the Westminster and Taneytown police, the Maryland State Police and the Sheriff's Office. A Civil Air Patrol plane circled overhead. Ian McHale, 17, who played a victim, said that the length of time taken to set up the response would have been unacceptable in a real−life situation. "If this was an emergency, we would be dead by now," he said. Organizers will review comments and gather criticisms. The county has 60 days to craft its formal assessment for Homeland Security officials.
Source: http://www.baltimoresun.com/news/local/carroll/bal−ca.drill19jun19,1,974110.story?coll=bal−local−carroll

25. *June 18, Beaver County and Allegheny Times (PA)* — **Pennsylvania home explosion prompts 911 notification bill.** When their Moon Township, PA, home exploded three months ago, the residents were stunned to learn that natural gas from a nicked pipeline had been filling the house for nearly two hours and that local emergency personnel had no idea anything was wrong. It is because of the March 16 explosion that U.S. Representative Tim Murphy introduced legislation Friday, June 17, requiring nationally that anyone who damages a pipeline immediately contact emergency responders and the owners of the pipeline. He said House Bill 2958, or the Pipeline Safety Emergency Notification Act, will be discussed in the House committees on transportation and energy and commerce. It will clearly spell out that workers should dial 911 where service is available as a way to notify emergency personnel. Under the proposed legislation, those who violate the law would be subject to a civil fine of up to $1 million and five years in prison.
House Bill 2958: http://thomas.loc.gov/cgi−bin/bdquery/D?d109:5:./temp/~bdyCLo:@@@L&summ2=m&
Source: http://www.timesonline.com/site/news.cfm?newsid=14721081&BRD=2305&PAG=461&dept_id=478569&rfi=6

26. *June 18, Associated Press* — **California will speed up disaster alert plan.** The California Office of Emergency Services will speed up implementation of a new system that will immediately alert individual county officials of tsunamis and other potential disasters. The agency's decision comes after emergency services officials in San Francisco and Sonoma County complained they were not notified quickly enough when the state tsunami alert was issued an earthquake off the Northern California coast Tuesday, June 14. San Francisco was delayed nearly an hour in activating its emergency plan, which included evacuating people near the shore. The new computerized warning system, which already had been in the pipeline, should be up and running within three months, said Henry Renteria, director of the Governor's Office of Emergency Services. The system will place simultaneous calls to designated officials statewide, sending messages to their cell phones, home phones, offices and any other numbers they specify. Currently, the state dispatches warnings via Teletype to county offices of emergency services, not to specific individuals.
OES Website: http://www.oes.ca.gov/Operational/OESHome.nsf/1?OpenForm

Source: http://www.dailynews.com/Stories/0,1413,200~20954~2928387,00 .html

[Return to top]

Information Technology and Telecommunications Sector

27. *June 20, Federal Computer Week* — **Office of Management and Budget modifies security reporting.** The Office of Management and Budget (OMB) has issued new security reporting guidelines that emphasize contractor oversight and data privacy protections. Under the 2005 Federal Information Security Management Act (FISMA) reporting guidelines issued Monday, June 13, agencies will have to answer new questions about data privacy and contractor oversight in reports they must submit to OMB by October 7. When OMB officials added the new questions, they also dropped some old ones. Agencies, for example, will no longer have to report how many times they were victims of a malicious code attack because someone in the agency had not installed a necessary security patch. The new guidelines emphasize that agencies are responsible for ensuring that federal contractors maintain appropriate security controls on equipment used to deliver network or other managed services. The security controls also apply to contractor support staff, government−owned and contractor−operated equipment and contractor−owned equipment in which any federal data is processed or stored. “Agencies must ensure identical, not equivalent security procedures,” according to the guidelines. That means agencies must make certain that federal contractors conduct risk assessments, develop contingency plans, certify and accredit their systems and everything else that federal agencies must do to comply with FISMA.
Source: http://www.fcw.com/article89321−06−20−05−Web

28. *June 20, eWeek.com* — **Drive−by download sites chauffeur spyware.** Increasingly, spyware is making its way onto users' systems through so−called drive−by−download sites using nefarious methods that circumvent disclosure. One example is iFrameDollars.biz, which claims to be a Website affiliate company just for drive−by sites, using a model similar to aboveboard affiliate networks such as Commission Junction and LinkShare. The Website's "Terms" page says that iFrameDollars.biz pays 55 cents per install or $55 for 1,000 unique installs of a three KB program that "changes the homepage and installs toolbar and dialer." Website operators interested in joining the iFrameDollars.biz network must submit a URL for their Websites, an estimate of their daily traffic and the account number for an online payment service such as E−gold. In exchange, they are sent a small piece of HTML code containing the iFrame exploit, which the site owners are expected to attach to their pages. Web surfers who visit those pages using vulnerable versions of Windows or Microsoft Corp.'s Internet Explorer Web browser have iFrameDollars.biz's programs silently installed. In addition to distributing malicious code and adware through its affiliates, iFrameDollars.biz uses pop−up messages to tempt users into buying nonexistent software programs, taking a cut of any sales.
Source: http://www.eweek.com/article2/0,1759,1829174,00.asp

29. *June 17, CNET News* — **Spyware and Adware in BitTorrent downloads.** Purveyors of the applications that produce pop−up ads on PC screens and track browsing habits have discovered BitTorrent as a new distribution channel. BitTorrent has grown into one of the most widely used means of downloading files such as movies or software. According to observers of the trend, videos and music that hide adware and spyware are increasingly being offered for

download on various BitTorrent Websites. Both spyware and adware are known to hurt PC performance because they use PC resources to run. Alex Eckelberry, president of Sunbelt Software, a maker of anti−spyware software stated: "[This] is a major concern. It is going to riddle your system with pop−ups, slow your system down and potentially cause system instability." The downloaded files typically were self−extracting archives that would also install the unwanted software, said Chris Boyd, a security researcher who runs the Vital Security Website. In most cases, users would be presented with a dialog box advising that the extra software was about to be installed and given the impression that the install was needed to get access to the desired content, he said.
Source: http://tech.nytimes.com/cnet/CNET_2100−7349_3−5750601.html

30. *June 17, Sun Microsystems* — **Sun ONE/iPlanet Messaging Server Webmail MSIE HTML injection vulnerability.** Sun ONE/iPlanet Messaging Server Webmail is prone to an HTML injection vulnerability. This issue may allow a remote attacker to inject hostile HTML and script code into the session of a Webmail user. Sun has stated that this issue only affects users who access Webmail with Internet Explorer. There is no solution at this time.
Source: http://sunsolve.sun.com/search/document.do?assetkey=1−26−101770−1

31. *June 17, Washington Technology* — **Retailers join Homeland Security Information Network.** Retailers are among the industry groups being invited to join a recent incarnation of the federal Homeland Security Information Network (HSIN) specifically intended for critical infrastructure owners and operators and designed to help share unclassified information to guard against terrorist attacks. The National Retail Federation (NRF) has recruited executives from nearly 100 retail companies to participate in the network, called HSIN−CL, the trade group said in a press release. The information network is a composite of several regional networks that share information among law enforcement, fire departments, local government agencies and businesses. Technologies used within the network include wired and wireless telephones, e−mail, facsimiles, and text pagers to share alerts and notifications. The network sends real−time information to its members, may be used “to discuss day−to−day security issues” and “to share information on suspicious activities with federal authorities” according to the NRF release. Other industry sectors, including the chemical industry, ports and financial services, are expected to participate in the HSIN−CL as well.
NRF news release: http://www.nrf.com/content/press/release2005/hsin0605.htm
Source: http://www.washingtontechnology.com/news/1_1/homeland/26420−1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Activity on one of the ports associated with Windows' Server Message Block (SMB) protocol is climbing. A surge in activity targeting TCP port 445, which is associated with SMB−related

communications on Windows machines has been observed. This may indicate an increase in known attacks, such as password brute forcing, or the exploitation of known vulnerabilities, or may indicate activity related to the recent Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability. Zone−H reported a rash of defacements of foreign .gov web pages today. US .gov web administrators should pay special attention to your servers. You could be targeted next.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 1026 (−−−), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 53 (domain), 137 (netbios−ns), 18152 (−−−), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer